AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH THE ACCOUNT OSCARBURGOS18@HOTMAIL.COM, STORED AT PREMISES CONTROLLED BY MICROSOFT

Case No. MJ18-342

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 371	Conspiracy
18 USC 2113(b)	Bank Theft

The application is based on these facts:

See Attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: ____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Julianna Dippold, Special Agent
Printed name and title

Sworn to before me pursuant to CrimRule 4.1.

Date: July 27, 2018

Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge
Printed name and title

AFFIDAVIT OF JULIANNA DIPPOLD

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, JULIANNA DIPPOLD, being first duly sworn on oath, depose and say:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been so employed since January 2018. I am currently assigned to the Vancouver, Washington Resident Agency of the Seattle, Washington Division.

2. Beginning in January 2018, I attended a 19-week training course at the FBI Academy. Before serving as a FBI Special Agent, I served as a sworn law enforcement officer with the United States Border Patrol where I investigated immigration-related offenses.

3. As a Special Agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THIS AFFIDAVIT

4. I make this affidavit in support of an application for a search warrant for information associated with the email account oscarburgos18@hotmail.com (hereinafter the "SUBJECT ACCOUNT") that is stored at premises controlled by Microsoft Corporation ("Microsoft"), an e-mail provider headquartered at One Microsoft Way in Redmond, Washington. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Microsoft to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

5. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that JOAO SILVA ROBERTSON, PEDRO LEON RIVERO VELAZQUEZ, STARLIN RAFAEL GARCIA CARABALLO, JOSSHOA PEREZ RIVAS, LUIS GERARDO MENDEZ MATA, JEAN DUMONT GONZALEZ, and CARLOS GONCALVES DURAN and others, (collectively, the "co-conspirators") have committed violations of Title 18, United States Code, Sections 371 (Conspiracy) and 2113(b) (Bank Theft). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment B.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. I have not included every fact known concerning this investigation. I have set forth the facts that I believe are necessary to determine probable cause for the requested search warrant.

III. JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." Additionally, the Court "is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored."

IV. SUMMARY

8. Beginning on December 13, 2017, five ATMs located in the Western District of Washington were jackpotted, resulting in losses exceeding $267,000. Jackpotting involves the installation of malware on ATMs, causing these ATMs to dispense their cash reserves.[1]

[1] All of these financial institutions were insured under the Federal Insurance Deposit Act or the National Credit Union Share Insurance Fund.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Date	Description
12/13/17	At least $88,000 stolen from a Sound Credit Union ATM located in Bothell, Washington by jackpotting.
12/15/17	At least $8,000 stolen from an IQ Credit Union ATM located in Vancouver, Washington by jackpotting.
12/16/17	At least $16,000 stolen from an Umpqua Bank ATM in Vancouver, Washington by jackpotting.
12/16/17	At least $91,000 stolen from a Columbia Credit Union ATM in Vancouver, Washington by jackpotting.
12/17/17	At least $64,400 stolen from a Heritage Bank ATM in Mount Vernon, Washington by jackpotting.

9. After reviewing surveillance images from these jackpotting attacks, information obtained pursuant to proffers, and information obtained from email search warrants, among other evidence, law enforcement determined that SILVA ROBERTSON, PEDRO LEON RIVERO VELAZQUEZ, STARLIN RAFAEL GARCIA CARABALLO, JOSSHOA PEREZ RIVAS, and LUIS GERARDO MENDEZ MATA were involved in the Washington jackpotting attacks.

10. As described herein, law enforcement is investigating whether Oscar David Burgos Guitian was involved in committing jackpotting[2] or skimming offenses, for the following reasons. Skimming involves the insertion of devices into ATMs in order to capture information from inserted credit and debit cards.

a. Two individuals arrested for jackpotting ATMs in Utah—CARLOS GONCALVES DURAN and JEAN DUMONT GONZALEZ—told SILVA ROBERTSON that their friend, "Oscar David," had created jackpotting malware. PEREZ RIVAS also stated that "Oscar David" told him he had jackpotting malware and discussed committing jackpotting attacks.[3]

[2] As described in detail below, SILVA ROBERTSON, GARCIA CARABALLO, and PEREZ RIVAS also stated that an individual named "Anibal" created the malware used during the jackpotting attacks in Washington. Law enforcement is also investigating the relationship, if any, between Oscar David Burgos Guitian and "Anibal."

[3] As stated in further detail below, PEREZ RIVAS also provided additional information that was inaccurate, causing law enforcement to question his credibility.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. PEREZ RIVAS' iCloud account contained screenshots of a conversation with "Oscar David," in which "Oscar David" described having jackpotting malware and requested that PEREZ RIVAS use the malware. According to the metadata associated with these screenshots, they were last modified on November 18, 2017—less than a month before the Washington jackpotting attacks began.

c. On November 28, 2017—less than three weeks before the Washington jackpotting attacks began—"Oscar Burgos" sent a package to Seattle, addressed to SILVA ROBERTSON's known alias, which purportedly contained "sensor sheets."

d. On December 1, 2017, GARCIA CARABALLO sent SILVA ROBERTSON a screenshot of a text communication with "Oscar David." "Oscar David" said he sent a photograph of his shipment, requested that they keep their expenses low, and said that he'd ordered a skimming device.

e. While the Washington jackpotting attacks were ongoing—from December 14, 2017 through December 18, 2017—PEREZ RIVAS transferred $10,000 from his Bank of America checking account to "Neomar Oscar David."

11. As described herein, the SUBJECT ACCOUNT was used by Oscar David Burgos Guitian to receive communications and funds from PEREZ RIVAS.

V. PROBABLE CAUSE

A. JACKPOTTING OFFENSES IN WASHINGTON

12. From at least December 13, 2017 through December 17, 2017, JOAO SILVA ROBERTSON, PEDRO LEON RIVERO VELAZQUEZ, STARLIN RAFAEL GARCIA CARABALLO, JOSSHOA PEREZ RIVAS, and LUIS GERARDO MENDEZ MATA jackpotted ATMs in the Western District of Washington. An example of one of these jackpotting attacks is described below.

1. JACKPOTTING IN VANCOUVER, WASHINGTON

13. On December 16, 2017, at least $91,000 was withdrawn from a Columbia Credit Union bank in Vancouver, Washington through jackpotting. According to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

surveillance images, at the beginning of this jackpotting attack, a car approached Columbia Credit Union's drive-through ATM and a passenger exited the vehicle.

14. While exiting the vehicle, the passenger—who I have identified as PEREZ RIVAS—appeared to have a small object in his hand. Based on my training and experience, and information gained during the course of this investigation, I understand that ATMs have at least two compartments, a top cover that conceals the internal computer and screen, and a bottom cover that conceals cassettes holding cash reserves. According to information obtained from Columbia Credit Union, the top cover of the ATM involved in this attack can be unlocked and opened using a key.

15. After exiting the vehicle, PEREZ RIVAS appeared to make hand motions consistent with turning a key and opening the top cover of the ATM, exposing its internal computer. While he was performing these tasks, white earbuds were visible in both of PEREZ RIVAS's ears, and PEREZ RIVAS appeared to be talking aloud, consistent with speaking to another via a cell phone.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

16. After approximately thirty seconds, the surveillance image abruptly cut-off and PEREZ RIVAS was no longer visible, consistent with the ATM being disconnected or taken offline.

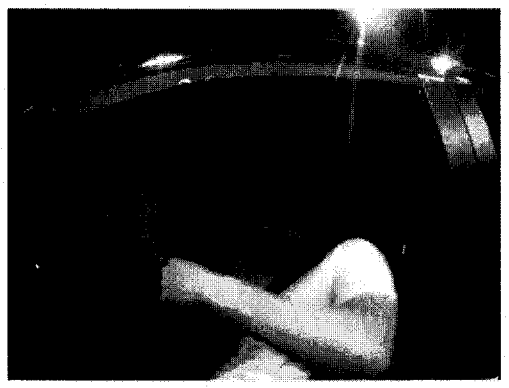
17. According to surveillance images obtained from another camera at Columbia Credit Union, during this time PEREZ RIVAS can be seen opening the top cover of the ATM and pulling the tray that contained the internal computer forward. Shortly thereafter, PEREZ RIVAS returned to the vehicle and the vehicle left the bank.

18. Approximately one minute later, the vehicle returned to the Columbia Credit Union ATM, and PEREZ RIVAS again appeared to open its cover before the vehicle departed and returned once more. Upon returning, the driver of the vehicle—who I have identified as GARCIA CARABALLO—was visible in the surveillance images. The ATM screen can also be seen in the reflection of the driver's side window, displaying a white screen with text.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

19. Approximately thirty seconds later, the ATM screen turned blue, displaying black and white text.

20. Approximately two minutes later, GARCIA CARABALLO began removing cash from the ATM. Based on my training and experience, and information gained during the course of this investigation, I understand that a jackpotted ATM will begin dispersing money after malware is installed.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

21. According to surveillance images, GARCIA CARABALLO collected money dispersed from the ATM for approximately twenty-seven minutes, each time handing stacks of cash to someone seated in the rear of the vehicle.

22. At the conclusion of the attack, PEREZ RIVAS again exited the vehicle and approached the ATM. PEREZ RIVAS appeared to make a hand motion consistent with opening the top cover of the ATM. At that point, the surveillance image abruptly cut-off and neither PEREZ RIVAS nor the car were visible, consistent with the ATM being disconnected or taken offline. The vehicle then left the bank and drove away.

23. On December 18, 2017, Columbia Credit Union contacted the Vancouver Police Department after discovering that its ATM was out of service. The bank called their ATM service provider, who found that the ATM was offline. Upon opening the ATM, the service provider found a USB plug inserted into the ATM's internal computer. The service provider also observed pry marks on the side of the ATM, near the key hole, and on the ATM hard drive's metal cover. Columbia Credit Union reported that at least $91,000 had been withdrawn from the ATM.

24. FBI collected the hard drive from the Columbia Credit Union ATM and submitted it for forensic examination. An FBI Computer Scientist concluded that the hard drive contained PLOUTUS-D, a malware variant. According to public reporting, and information obtained from other attacks, PLOUTUS-D has previously been used in jackpotting attacks in Latin America and the United States.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

25. As described in further detail below, on February 25, 2018, STARLIN RAFAEL GARCIA CARABALLO and JOSSHOA PEREZ RIVAS were arrested in Sandy, Utah. After their arrests, I obtained photographs of these individuals and confirmed that GARCIA CARABALLO was the driver, and PEREZ RIVAS was the passenger, observed in the Columbia Credit Union surveillance images.

B. JACKPOTTING OFFENSES IN UTAH

26. In addition to jackpotting in Washington, SILVA ROBERTON, RIVERO VELAZQUEZ, GARCIA CARABALLO, PEREZ RIVAS, MENDEZ MATA, DUMONT GONZALEZ, and GONCALVES DURAN also jackpotted ATMs in Utah in February 2018.

27. On February 23, 2018, PEREZ RIVAS, GARCIA CARABALLO, RIVERO VELAZQUEZ, and MENDEZ MATA were observed by law enforcement arriving at the Salt Lake City International Airport and meeting with SILVA ROBERTSON. After arriving, a number of these individuals rented vehicles. Law enforcement officers surveilled these individuals after they departed the airport, and saw them meeting in the subsequent days with GONCALVEZ DURAN and DUMONT GONZALEZ.

28. On February 25, 2017, a car rented by RIVERO VELAZQUEZ drove to the Deseret First Credit Union ATM in Sandy, Utah. Thereafter, the ATM displayed a screen that indicated the software system of the ATM had been breached. As law enforcement agents approached RIVERO VELAZQUEZ's vehicle, the ATM was dispensing cash. Agents arrested four individuals, later identified as SILVA ROBERTSON, GARCIA CARABALLO, RIVERO VELAZQUEZ, and PEREZ RIVAS. Agents also located electronic equipment and a bag of cash in the vehicle, and recovered multiple cell phones, including SILVA ROBERTSON's iPhone.

29. After the attack, a technician examined the ATM and located a dongle, used to attach a keyboard to the ATM computer, as well as cables and two hard drives.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Additionally, the compartment covering the ATM's hard drive appeared to have been forcefully opened.

30. According to witnesses, MENDEZ MATA was in a vehicle parked at a gas station nearby for the purpose of monitoring the progress of the jackpotting from a distance. Law enforcement was unable to apprehend MENDEZ MATA, who left before he could be arrested.

31. GONCALVEZ DURAN and DUMONT GONZALEZ were also located in the vicinity of the Deseret First Credit Union ATM but escaped arrest. They were apprehended on March 3, 2018, as they attempted to leave the country on planes departing from Miami, Florida.

C. SILVA ROBERTSON PROFFER

32. In a proffer interview, conducted on March 8, 2018, SILVA ROBERTSON explained that GONCALVES DURAN and DUMONT GONZALEZ were in Washington before traveling to Utah. While in Washington, GONCALVES DURAN and DUMONT GONZALEZ told SILVA ROBERTSON that their friend, "Oscar David," had created jackpotting malware.

33. SILVA ROBERTSON told GONCALVES DURAN and DUMONT GONZALEZ that he was involved in jackpotting and invited GONCALVES DURAN and DUMONT GONZALEZ to Utah to jackpot with RIVERO VELAZQUEZ, GARCIA CARABALLO, PEREZ RIVAS, and MENDEZ MATA.

34. SILVA ROBERTSON also stated that RIVERO VELAZQUEZ, GARCIA CARABALLO, PEREZ RIVAS, and MENDEZ MATA jackpotted ATMs in Washington in December 2017.

35. SILVA ROBERTSON explained that an individual named "Anibal" created the malware that was used to jackpot ATMs in Utah and Washington. SILVA ROBERTSON never met or spoke to "Anibal."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

D. GARCIA CARABALLO PROFFER

36. In a proffer interview, conducted on May 31, 2018, GARCIA CARABALLO explained that SILVA ROBERTSON invited GARCIA CARABALLO and RIVERO VELAZQUEZ to Seattle, Washington to engage in skimming. When the skimming devices failed to arrive, PEREZ RIVAS contacted GARCIA CARABALLO and told him that he had some work for GARCIA CARABALLO.

37. GARCIA CARABALLO explained that an individual named "Oscar" previously had introduced him to PEREZ RIVAS in Orlando, Florida. MENDEZ MATA was also present with "Oscar" in Florida.

38. GARCIA CARABALLO, SILVA ROBERTSON, and RIVERO VELAZQUEZ met with PEREZ RIVAS, who was traveling with MENDEZ MATA, in Seattle, Washington. When they met, PEREZ RIVAS described how to jackpot an ATM. GARCIA CARBALLO was told that he would serve as a driver and lookout while the attacks were being conducted.

39. GARCIA CARABALLO was told that an individual named "Anibal" owned the jackpotting malware. GARCIA CARABALLO never met or spoke to "Anibal."

E. PEREZ RIVAS PROFFER

40. In a proffer interview, conducted on June 21, 2018, PEREZ RIVAS explained that he came from Mexico to the United States in June 2017. After arriving in the United States, he engaged in skimming—including skimming in California in or around July and August 2018—and jackpotting ATMs.

41. PEREZ RIVAS explained that he has known "Oscar David" for approximately six years, and that he is involved in skimming ATMs in the United States. PEREZ RIVAS stated that "Oscar David" and "Anibal" also know one another. PEREZ RIVAS claimed that "Oscar David" could engage in jackpotting through "Anibal" and acknowledged receiving text messages from "Oscar David" regarding jackpotting,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

including the text conversation described below, last modified on November 18, 2017—less than a month before the Washington jackpotting attacks began.

42. PEREZ RIVAS claimed that he sent in funds to "Oscar David" in December 2017 in order to purchase a car in Venezuela. When asked why he would need a car in Venezuela, since PEREZ RIVAS lived in Mexico and claimed to have limited funds, PEREZ RIVAS stated that he might return to Venezuela in the future. PEREZ RIVAS claimed that he never engaged in jackpotting with "Oscar David." PEREZ RIVAS provided other information, which he later confirmed was inaccurate, including initially claiming that he didn't know "Anibal" and then later stating that "Anibal" was responsible for the Washington jackpotting attacks. PEREZ RIVAS also initially claimed that MENDEZ MATA explained jackpotting after PEREZ RIVAS arrived in Chicago in December 2017, later stating that MENDEZ MATA spoke to him about jackpotting while they were both in Mexico. As a result, law enforcement believes that the information provided by PEREZ RIVAS may not be credible and, for the purpose of this warrant application, I am only relying upon statements made by PEREZ RIVAS that can be corroborated by external evidence.

F. PEREZ RIVAS' ICLOUD ACCOUNT

43. On May 3, 2018, law enforcement obtained a warrant to search the iCloud account associated with josshoaflames10@gmail.com. According to information obtained from Apple, the josshoaflames10@gmail.com iCloud account was registered to PEREZ RIVAS.

44. A screenshot of an Apple Notes page was contained in the iCloud account. According to the metadata associated with this screenshot, it was last modified on August 16, 2017. The note listed the name Oscar David Burgos Guitian, an account number at Bank of America, an address in Miami, Florida, and the email address oscarburgos18@hotmail.com (the SUBJECT ACCOUNT).

45. Screenshots of text communications with "Oscar David" were also contained in the iCloud account. According to the metadata associated with these

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

screenshots, they were last modified on November 18, 2017—less than a month before the Washington jackpotting attacks began. In these text communications, "Oscar David" stated that he had jackpotting software. The recipient of this text communication, believed to be PEREZ RIVAS, asked about the installation. The two also discussed which brands of ATMs the jackpotting software would work on, and "Oscar David" asked PEREZ RIVAS where to send the laptops.

46. The iCloud account also contained screenshots of communications with "Anibal." According to the metadata associated with these screenshots, they were last modified on November 17, 2017. In these communications "Anibal" and a second person, believed to be PEREZ RIVAS, discussed arrests, believed to be the arrests in Wyoming of individuals suspected of jackpotting ATMs.

47. Lastly, the iCloud account contained screenshots of communications with "Anibal New." According to the metadata associated with these screenshots, there were last modified on November 17, 2017. In these communications, an individual, believed to be PEREZ RIVAS, described a trip happening the following week. It is unclear whether this trip is linked to the jackpotting attacks that occurred in Washington in December 2017.

G. DHL SHIPMENT

48. According to information obtained from DHL, on November 28, 2017—less than three weeks before the Washington jackpotting attacks began—"Oscar Burgos" sent Paolo Pucci a package. Based on information gained during the course of this investigation, I know that Paolo Pucci is an alias used by SILVA ROBERTSON. The package was sent from Caracas, Venezuela and addressed to a FedEx store in Seattle, Washington. The contents of the package were described as "sensor sheets" and the package weighed ½ kilogram.

H. SILVA ROBERTSON'S CELL PHONE

49. According to information obtained from SILVA ROBERTSON's cell phone, seized upon his arrest and searched pursuant to consent, in November 2017

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

GARCIA CARABALLO and SILVA ROBERTSON exchanged multiple text messages.

a. For example, on November 14, 2017, GARCIA CARABALLO sent SILVA ROBERTSON a photograph of RIVERO VELAZQUEZ's passport. Three days later, on November 17, 2017, GARCIA CARABALLO sent SILVA ROBERTSON a photograph of GARCIA CARABALLO's passport.

c. On November 21, 2017, GARCIA CARABALLO told SILVA ROBERTSON to send him an address so he could send "las cosas," which translates into English as "the things." In response, SILVA ROBERTSON sent the address for the FedEx store in Seattle, Washington, listing the name Paolo Pucci.

d. On November 21, 2017, SILVA ROBERTSON sent GARCIA CARABALLO pictures of plane tickets for GARCIA CARABALLO and RIVERO VELAZQUEZ to fly from Lima, Peru to Miami, Florida.

e. On November 28, 2017, SILVA ROBERTSON again sent GARCIA CARABALLO the address for the FedEx store in Seattle, Washington.

f. On November 28, 2017, GARCIA CARABALLO sent SILVA ROBERTSON pictures of a skimming devices.

g. On December 1, 2017, GARCIA CARABALLO sent SILVA ROBERTSON a screenshot of a text communication with "Oscar David." "Oscar David" said he sent a photograph of his shipment, requested that they keep their expenses low, and said that he'd ordered a skimming device.

h. On December 7, 2017, GARCIA CARABALLO sent SILVA ROBERTSON a screenshot of a DHL shipment summary, showing that the package sent by "Oscar David," described above, arrived at in Seattle, Washington.

I. PEREZ RIVAS' BANK OF AMERICA ACCOUNT

50. According to documents obtained from Bank of America, PEREZ RIVAS opened checking and savings accounts on June 10, 2017.

51. Deposits and withdrawals were made from these accounts in December 2017, including the following:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. From December 14, 2017 through December 17, 2017, PEREZ RIVAS deposited $32,480 into his checking account at bank branches and ATMs in Washington.

b. From December 14, 2017 through December 18, 2017, $10,000 was transferred—in five separate transactions—from PEREZ RIVAS' checking account to "Neomar Oscar David."

c. These deposits and withdrawals were made during the same time period as the Washington jackpotting attacks, which occurred from December 13, 2017 through December 17, 2017.

52. Deposits and withdrawals were also made from this account in August 2017, including the following:

a. On August 7, 2017, PEREZ RIVAS also sent $1,016—in two separate transactions—from his savings account at Bank of America to "Oscar David." Both of these transfers are listed on PEREZ RIVAS' account statement as "Mobile/Email Transfer[s]."

b. From August 14-18, 2017, "Oscar Guitian" transferred $1,100—in two separate transactions—to PEREZ RIVAS' checking account at Bank of America. Law enforcement is investigating whether these transfers were initiated to return the funds sent by PEREZ RIVAS to Oscar David Burgos Guitian on August 7, 2017.

c. As described above, these funds were sent and received in August 2017, during the time period when PEREZ RIVAS was involved in skimming ATMs in California.

J. JOSSHOAFLAMES10@GMAIL.COM

53. According to information obtained from Google in response to a search warrant, the email account josshoaflames10@gmail.com was opened by JOSSHOA ANGEL PEREZ RIVAS on July 30, 2013.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

54. This account—josshoaflames10@gmail.com—contains numerous emails addressed to PEREZ RIVAS, including emails sent from Bank of America related to transfers from PEREZ RIVAS' accounts to "Neomar Oscar David" and "Oscar David."

a. For example, on December 14, 2017, Bank of America sent an email to josshoaflames10@gmail.com, describing a $2,499 transfer to "Neomar Oscar David" at the email address neomarblandin1@hotmail.com.

b. Additionally, on August 5, 2017, Bank of America sent an email to josshoaflames10@gmail.com, describing a $1,000 transfer to "Oscar David" at the email address oscarburgos18@hotmail.com (the SUBJECT ACCOUNT).

55. The josshoaflames10@gmail.com account also contained emails describing travel reservations with or related to Oscar David Burgos Guitian.

a. On October 17, 2016, josshoaflames10@gmail.com received an email describing a flight from Mexico City to Monterrey, Mexico, scheduled to depart that same day. The passengers on the Interjet 220 flight were listed as LUIS GERARDO MENDEZ MATA, "Oscar David Burgos," JOSSHOA PEREZ, and a fourth individual unknown to law enforcement.

b. One month prior, on September 23, 2016, an email was sent from josshoaflames10@gmail.com to oscarburgos18@hotmail.com (the SUBJECT ACCOUNT) attaching a flight itinerary for an unknown passenger traveling from Bogota, Columbia to Mexico City, Mexico.

K. INFORMATION ABOUT MOBILE TRANSFERS

56. According to information available at www.bankofamerica.com,[4] a Bank of America account holder can send funds to another by initiating a transfer through Bank of America's mobile application. The account holder would add a recipient and enter either the recipient's email address or mobile telephone number. The account holder could then

[4] https://www.bankofamerica.com/onlinebanking/education/how-to-send-money-online.go and https://promo.bankofamerica.com/zelle/.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

determine the amount of funds to transfer and initiate the transfer. The recipient will receive a notification by text or email, depending on the information input by the sender for that recipient. If the recipient is not a Bank of America customer that email will also contain instructions on how to register to receive the transferred funds.

57. Accordingly, I believe that when PEREZ RIVAS sent funds from his Bank of America account to "Oscar David," listing the email address oscarburgos18@hotmail.com, that Bank of America would send a transfer notification to the SUBJECT ACCOUNT.

L. CONCLUSION

58. Accordingly, as explained herein, there is probable cause to believe that the SUBJECT ACCOUNT contains evidence, fruits, or instrumentalities related to the crimes under investigation.

59. Specifically, as explained by SILVA ROBERTSON and PEREZ RIVAS, and as indicated in text communications found in PEREZ RIVAS' iCloud account, "Oscar David" claimed to possess malware that can be used to jackpot ATMs. PEREZ RIVAS also stated that "Oscar David" was involved in skimming ATMs in the United States.

60. Before the Washington jackpotting offenses occurred, "Oscar David" sent text communications stating that he was sending a package to Seattle and claiming that he had ordered a skimming device. That package, addressed to a known alias for SILVA ROBERTSON, arrived in Seattle one week before the Washington jackpotting offenses occurred.

61. While the jackpotting attacks were ongoing, PEREZ RIVAS sent $10,000, in four separate transactions, to "Neomar Oscar David." Before that date, while PEREZ RIVAS was skimming ATMs in California, PEREZ RIVAS sent additional funds to "Oscar David."

62. PEREZ RIVAS communicated with Oscar David Burgos Guitian using the SUBJECT ACCOUNT, sending him an email related to travel in 2016, and saving an

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Apple Note listing Oscar David Burgos Guitian's banking details, address, and the SUBECT ACCOUNT in his iCloud account. In August 2017, PEREZ RIVAS also sent funds to "Oscar David" listing the SUBJECT ACCOUNT via a mobile/email transfer, which, based on information obtained from Bank of America, would likely have generated an email to the SUBJECT ACCOUNT confirming the sending of those funds.

63. On April 20, 2018, the government sent a preservation request for the SUBJECT ACCOUNT to Microsoft. Accordingly, information exists in the stored content information regarding these accounts, which is available through Microsoft.

VI. BACKGROUND CONCERNING E-MAIL

64. In my training and experience, I have learned that Microsoft provides a variety of on-line services, including electronic mail ("e-mail") access, to the public. Microsoft allows subscribers to obtain e-mail accounts at the domain name @hotmail.com, like the e-mail account listed in Attachment A. Subscribers obtain an account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, the computers of Microsoft are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Microsoft subscribers) and information concerning subscribers and their use of Microsoft services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

65. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

under investigation because the information can be used to identify the account's user or users.

66. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

67. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

68. As explained herein, information stored in connection with an e-mail account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an e-mail account can indicate who has used or controlled the account. This "user attribution" evidence is

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, e-mail communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the e-mail provider can show how and when the account was accessed or used. For example, as described below, e-mail providers typically log the Internet Protocol (IP) addresses from which users access the e-mail account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the e-mail account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via e-mail). Last, stored electronic data may provide relevant insight into the e-mail account owner's state of mind as it relates to the offense under investigation. For example, information in the e-mail account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

69. In my training and experience, an e-mail that is sent to a Microsoft subscriber is stored in the subscriber's "mail box" on Microsoft servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Microsoft servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Microsoft servers for a certain period of time.

VII. REQUEST FOR SEALING

70. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed as described in the attached sealing motion. These documents discuss an ongoing criminal investigation that is not known to all of the targets of the investigation, at least one target of the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

investigation is a fugitive and believed to be located abroad, and the evidence described herein includes proffer statements that have not been revealed. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

VIII. CONCLUSION

71. Based on the information set forth herein, I believe probable cause exists to search the SUBJECT ACCOUNT, described in Attachment A, for evidence, fruits and instrumentalities, as further described in Attachment B, of crimes committed by JOAO SILVA ROBERTSON, PEDRO LEON RIVERO VELAZQUEZ, STARLIN RAFAEL GARCIA CARABALLO, LUIS GERARDO MENDEZ MATA, JOSSHOA PEREZ RIVAS, JEAN DUMONT GONZALEZ, CARLOS GONCALVES DURAN, Oscar David Burgos Guitian, and others, specifically, violations of Title 18, United States Code, Sections 371 (Conspiracy) and 2113(b) (Bank Theft).

72. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Microsoft who will then compile the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

JULIANNA DIPPOLD
SPECIAL AGENT

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit on 27 day of July, 2018.

HONORABLE MARY ALICE THEILER
UNITED STATES MAGISTRATE JUDGE

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Property to Be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with the Microsoft account oscarburgos18@hotmail.com (the "Account") that is stored at a premises controlled by Microsoft, a company that accepts service of legal process at One Microsoft Way in Redmond, Washington.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

Particular Things to be Seized

I. Section I - Information to be Disclosed by Microsoft (the "Provider"):

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all e-mails associated with the accounts, including stored or preserved copies of e-mails sent to and from the accounts, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the IP address used to register the accounts, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the accounts, including contacts with support services and records of actions taken.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to be Seized by the Government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 371 (Conspiracy) and 2113(b) (Bank Theft), those violations involving JOAO SILVA ROBERTSON, PEDRO LEON RIVERO VELAZQUEZ, STARLIN RAFAEL GARCIA CARABALLO, JOSSHOA PEREZ RIVAS, LUIS GERARDO MENDEZ MATA, JEAN DUMONT GONZALEZ, and CARLOS GONCALVES DURAN, Oscar David Burgos Guitian, or others, those violations occurring between January 2017 and the present, including content created between January 2017 and the present, for the Account listed on Attachment A, and any linked accounts, including the following:

a. Any content that may identify any alias names or online user names, of those who exercise in any way any dominion or control over the accounts as well as records or information that may reveal the true identities of these individuals;

b. Any records or information showing the location from which the account user has accessed or utilized the account, including GPS, Wi-Fi, or cell tower proximity records related to the account;

c. Any lists of linked accounts;

d. Any subscriber records for accounts or linked accounts;

e. Any address lists or buddy/contact lists associated with the accounts;

f. All calendars associated with the accounts;

g. Any records of communications between Microsoft, and any person about issues relating to the accounts, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

h. Any content relating to who created, used, or communicated with the account, including records about their identities and whereabouts;

i. Any content concerning creating, obtaining, or using malware;

j. Any content concerning jackpotting ATMs;

k. Any content concerning acquiring, installing, or using equipment to jackpot ATMs;

l. Any content concerning acquiring, installing, or using any technology or hardware designed to steal funds or information from ATMs, including skimming devices that could be installed on ATMs or other point of sale devices;

m. Any content concerning identification of locations to commit legal offenses;

n. Any content that may identify travel patterns or car, hotel, and airline reservations of co-conspirators or those using the accounts;

o. Any content that may identify payment information used during the legal offenses;

p. Any content concerning payments made by co-conspirators during the time of the legal offenses;

q. Any content concerning co-conspirators or that may reveal the identities of co-conspirators and the relationship amongst co-conspirators;

r. Any content concerning methods of communicating with co-conspirators, including telephone, text message, email or other means of communication;

s. Any content concerning the victims of these legal offenses;

t. Any content concerning efforts to evade law enforcement or to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of these legal offenses;

u. Any content that may identify assets including bank accounts, commodities accounts, trading accounts, personal property and/or real estate that may represent proceeds of these legal offenses; and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

v. Any content concerning the account user's state of mind as it relates to the crimes under investigation.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Microsoft, Inc., and my official title is _____. I am a custodian of records for Microsoft Corporation. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Microsoft, Inc. and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Microsoft Corporation.; and

c. such records were made by Microsoft Corporation. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date Signature

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970